

1 David. S. Casey, Jr., SBN 060768
2 *dcasey@cglaw.com*
3 Gayle M. Blatt, SBN 122048
4 *gmb@cglaw.com*
5 P. Camille Guerra, SBN 326546
6 *camille@cglaw.com*
7 **CASEY GERRY SCHENK**
8 **FRANCAVILLA BLATT & PENFIELD, LLP**
9 110 Laurel Street
10 San Diego, CA 92101
11 Tel: (619) 238-1811
12 Fax: (619) 544-9232

13 *Attorneys for Plaintiffs and
the Putative Classes
[Additional Counsel Listed on Signature Page]*

14 **UNITED STATES DISTRICT COURT**

15 **NORTHERN DISTRICT OF CALIFORNIA**

16 MICHAEL GREENSTEIN and
17 CYNTHIA NELSON, on behalf of
18 themselves and all other persons
19 similarly situated,

20 Plaintiffs,

21 v.

22 NOBLR RECIPROCAL EXCHANGE, a
23 Delaware corporation,

24 Defendant.

25 Case No. 3:21-cv-4537

26 **CLASS ACTION COMPLAINT**

27 **Demand for Jury Trial**

28 Plaintiffs Michael Greenstein, and Cynthia Nelson, individually, and on behalf
of all others similarly situated, upon personal knowledge of facts pertaining to them
and on information and belief as to all other matters, by and through undersigned
counsel, hereby bring this Class Action Complaint against Defendant Noblr
Reciprocal Exchange and allege as follows:

1

2 **INTRODUCTION**

3 1. Every year millions of Americans have their most valuable personal
 4 information stolen and sold online because of unauthorized data disclosures. Despite
 5 warnings about the severe impact of unauthorized data disclosures on Americans of
 6 all economic strata, companies still fail to put adequate security measures in place to
 7 prevent the unauthorized disclosure of private data about their customers or potential
 8 customers.

9 2. Defendant Noblr Reciprocal Exchange (“Defendant” or “Noblr”),
 10 provides insurance products, including car insurance, to Americans across the
 11 country. In doing so, it promises “[y]ou trust us with your information and we are
 12 committed to keeping that trust,” “the security of your personal information is
 13 extremely important to us” and further promises in bold lettering “[w]e do not share
 14 your data or information without your permission.”¹

15 3. Noblr failed to meet these promises and its obligation to protect the
 16 sensitive personal information entrusted to it.

17 4. As reported by Noblr, on or about January 21, 2021, it “noticed unusual
 18 quote activity consisting of a spike in unfinished quotes through its instant quote
 19 webpage.” It launched an investigation and learned that “attackers may have
 20 initiated these quotes in order to steal driver’s license numbers which were
 21 inadvertently included in the page source code.”² This means that for an unknown
 22 period of time before and including January 21, 2021, the drivers’ license
 23 information of Plaintiffs and members of the class was publicly available via the
 24 page source code on Noblr’s public website and being stolen by hackers.

25

26

27 ¹ <https://www.noblr.com/privacy-policy/>

28 ² <https://media.dojmt.gov/wp-content/uploads/noblr-notif.pdf> (last visited May 29,
 2021).

5. As a corporation doing business in California, Noblr is legally required to protect the personal information (“PI”) it gathers from unauthorized access and exfiltration.

6. As a result of Noblr's failure to provide reasonable and adequate data security, Plaintiffs' and the Class Members' PI has been exposed to those who should not have access to it. Plaintiffs and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after private PI stolen here.

THE PARTIES

7. Defendant Noblr Reciprocal Exchange is a Delaware corporation with its principal place of business in Mill Valley, California. Noblr is an insurance provider currently providing insurance in Arizona, Colorado, Ohio, Louisiana, Maryland, Pennsylvania, New Mexico, and Texas, and has insurance licenses in all fifty states.

8. Plaintiff Michael Greenstein is a resident of Watchung, New Jersey. On or about May 2021, Plaintiff Greenstein received notice from Noblr that it improperly exposed his PI to unauthorized third parties. Plaintiff Greenstein never sought a quote for insurance of any sort from Defendant.

9. Plaintiff Cynthia Nelson is a resident of Watertown, Massachusetts. On or about May 2021, Plaintiff Nelson received notice from Noblr that it improperly exposed her PI to unauthorized third parties. Plaintiff never sought a quote for insurance of any sort from Defendant.

JURISDICTION AND VENUE

10. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds \$5 million, exclusive of interest and costs. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims and supplemental jurisdiction over the state law claims

1 pursuant to 28 U.S.C. § 1367.

2 11. This Court has personal jurisdiction over Defendant because it maintains
3 its principal place of business in this District, is registered to conduct business in
4 California, and has sufficient minimum contacts with California.

5 12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because
6 Defendant resides in this District and on information and belief, a substantial part of
7 the events or omissions giving rise to Plaintiffs' and Class Members' claims
8 occurred in this District.

9 13. Application of California law to this dispute is proper because
10 Defendant's headquarters are in California, the decisions, actions, and/or
11 circumstances that gave rise to the underlying facts at issue in this Complaint were
12 presumably made or taken in California, and the action and/or inaction at issue
13 emanated from California.

14 **INTRADISTRICT ASSIGNMENT**

15 14. Pursuant to Civil L.R. 3-1 (c) and (d), assignment to the San Francisco
16 Division is proper because a substantial part of the conduct which gives rise to
17 Plaintiffs' claims occurred in this district and specifically Marin County where
18 Defendant is headquartered.

19 **FACTUAL ALLEGATIONS**

20 **A. Noblr collects PI and fails to provide adequate data security**

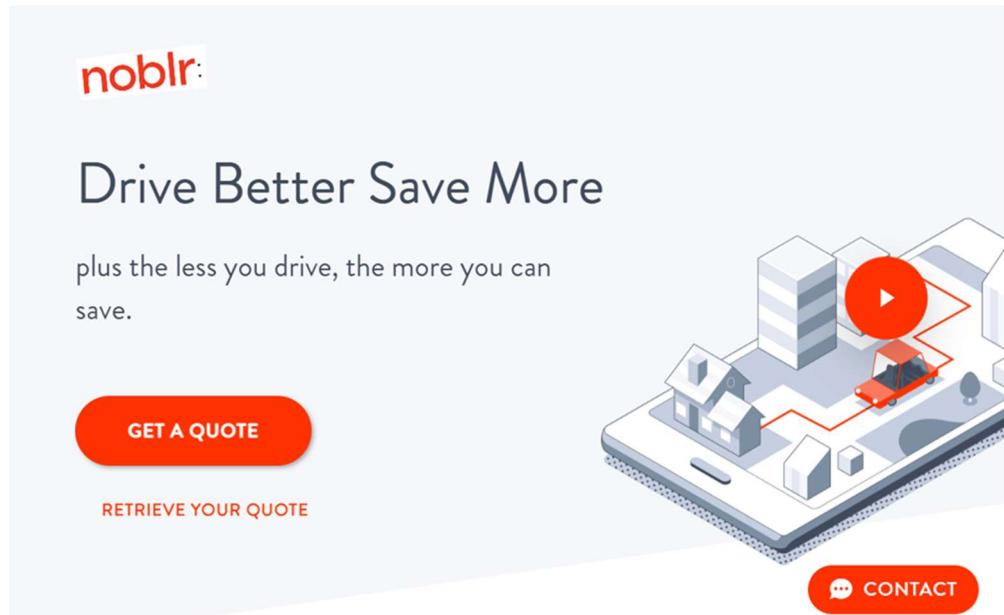
21 15. Noblr began as a car insurance start-up utilizing technology to provide a
22 product to attract good drivers, "Using behaviour based pricing, Noblr calculated
23 insurance premiums in real-time based on how a driver performs."³

24 16. Noblr currently offers various types of insurance policies, including auto,

27 ³ <https://www.artemis.bm/news/hudson-structured-invests-in-auto-insurtech-noblr/>
28 (last visited May 29, 2021).

1 renters, home and condo, and umbrella.⁴

2 17. Like other insurance providers, Noblr offers a public-facing insurance
3 quoting platform for visitors on its website. Visitors to Noblr's website can "Get A
4 Quote" instantly after providing personal information.



18 18. Noblr's quoting feature uses the information entered by the website's
19 visitor, combines it with additional information the system matches, and then
20 automatically pulls information from a third-party to provide the visitor a quote.

21 19. Unfortunately, Noblr's online quote system was configured to allow
22 anyone with a few basic bits of data to get Noblr's system to auto-fill the remaining
23 information, including driver's license numbers, from its databases, thus allowing
24 hackers to steal that information.

25 20. On or around January 21, 2021, Noblr finally realized that its instant
26 quote feature was being exploited by hackers who were using it to obtain the driver's
27 license numbers and addresses of Plaintiffs and the members of the Class, which
28 includes many people who never applied for insurance with Noblr or were even
aware of its existence.

⁴ <https://www.noblr.com/coverages/>

1 21. This incident is referred to herein as the “Unauthorized Data Disclosure.”

2 22. The named Plaintiffs received a letter from Noblr entitled “Notice of
3 Data Security Incident Involving Your Personal Data,” dated May 14, 2021. The
4 letter stated that their PI, detailed below, may have been compromised, and included
5 the following:

6 **What Happened**

7 On January 21, 2021, Noblr’s web team noticed unusual quote activity
8 consisting of a spike in unfinished quotes through its instant quote web
9 page. Noblr immediately launched an internal investigation. The initial
10 investigation revealed that attackers may have initiated these quotes in
11 order to steal driver’s license numbers which were inadvertently
included in the page source code.

12 As described above, the instant quote process works by taking personal
13 data (name and date of birth) entered into the system and matching it
14 with related information automatically pulled from a third-party to help
15 provide a quote. The attackers appear to have already been in
16 possession of the names and dates of birth of consumers, and then used
17 that information to obtain additional personal information through
18 Noblr’s instant quote platform. Attackers could also have gone through
the entire quote process to access personal information in the final
policy application documents provided after obtaining a quote.

19 On January 25, 2021, following the initial discovery of unusual quote
20 activity, Noblr’s security team began blocking suspicious IP addresses.
21 On January 27, 2021, when Noblr determined that the attackers were
22 able to access driver’s license numbers, Noblr altered its instant quote
system to prevent further access by the attackers and took other steps
to combat these attacks.

23 **What Information Was Involved**

24 Our records indicate that your name, driver’s license number, and
25 address may have been accessed.

26 **Actions We’ve Taken to Safeguard Your Information**

1 We take our responsibility to safeguard your personal information
 2 seriously. We immediately took steps to remedy the situation, including
 3 blocking suspicious IP addresses, revising rate limit thresholds to adjust
 4 specific traffic patterns, and altering the instant quote system to mask
 5 driver's license numbers in the source code and in the final application
 6 page. In addition, we are developing and employing certain changes to
 processes and protocols to prevent this type of event from happening
 again.⁵

7 23. The Notice confirms that Plaintiffs became victims of the Unauthorized
 8 Data Disclosure even though they did not have a prior relationship with Noblr,
 9 advising "you may be affected even if you have no relationship with Noblr if your
 10 information, or the information of someone in your household, was used by the
 11 attackers in connection with this incident."

12 24. After receiving Unauthorized Data Disclosure notice letters, it is
 13 reasonable for Plaintiffs and Class Members in this case to believe that the risk of
 14 future harm (including identity theft) is substantial and imminent, and to take steps
 15 to mitigate that substantial risk of future harm. In fact, in Noblr's letter it encourages
 16 affected individuals to use the identity theft protection service it offers to Plaintiffs
 17 and the Class to help protect their "identity from misuse" and that they should,
 18 among other things, "regularly review statements from your accounts and
 19 periodically obtain your credit report."

20 **B. The PI exposed by Noblr as a result of its inadequate data security is
 21 highly valuable on the black market**

22 25. The information exposed by Noblr is very valuable to phishers, hackers,
 23 identity thieves and cyber criminals, especially at this time where unprecedented
 24 numbers of fraudsters are filing fraudulent unemployment benefit claims.

25
 26 ⁵ Noblr's *Notice of Data Security Incident Involving Your Personal Information*, as
 27 filed with the Maine Attorney General,
 28 <https://apps.web.maine.gov/online/aewviewer/ME/40/c43bf2a1-cea9-45fa-81bf-47d299a7216d.shtml> (last visited on May 29, 2021).

1 26. Cybercrime has been on the rise for the past decade and continues to
 2 climb exponentially; as of 2013 it was being reported that nearly one out of four data
 3 breach notification recipients become a victim of identity fraud.⁶

4 27. Stolen PI is often trafficked on the “dark web,” a heavily encrypted part
 5 of the Internet that is not accessible via traditional search engines. Law enforcement
 6 has difficulty policing the dark web due to this encryption, which allows users and
 7 criminals to conceal identities and online activity.

8 28. When malicious actors infiltrate companies and copy and exfiltrate the PI
 9 that those companies store, or have access to, that stolen information often ends up
 10 on the dark web because the malicious actors buy and sell that information for
 11 profit.⁷

12 29. For example, when the U.S. Department of Justice announced its seizure
 13 of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which
 14 concerned stolen or fraudulent documents that could be used to assume another
 15 person’s identity. Other marketplaces, similar to the now-defunct AlphaBay, “are
 16 awash with [PI] belonging to victims from countries all over the world. One of the
 17 key challenges of protecting PI online is its pervasiveness. As unauthorized data
 18 disclosures in the news continue to show, PI about employees, customers and the
 19 public is housed in all kinds of organizations, and the increasing digital
 20 transformation of today’s businesses only broadens the number of potential sources
 21 for hackers to target.”⁸

22
 23 ⁶ Pascual, Al, “2013 Identity Fraud Report: Data Breaches Becoming a Treasure
 24 Trove for Fraudsters,” *Javelin* (Feb. 20, 2013).

25 ⁷ *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28,
 26 2020, available at: <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring> (last visited May. 29, 2021).

27 ⁸ *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor,
 28 April 3, 2018, available at: <https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/> (last visited June 10, 2021).

1 30. The PI of consumers remains of high value to criminals, as evidenced by
 2 the prices they will pay through the dark web. Numerous sources cite dark web
 3 pricing for stolen identity credentials. For example, personal information can be sold
 4 at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to
 5 \$200⁹. Experian reports that a stolen credit or debit card number can sell for \$5 to
 6 \$110 on the dark web¹⁰.

7 31. The information compromised in the Unauthorized Data Disclosure is
 8 significantly more valuable than the loss of, for example, credit card information in a
 9 retailer data breach because, there, victims can cancel or close credit and debit card
 10 accounts. The information compromised in this Unauthorized Data Disclosure is
 11 difficult and likely highly problematic, to change—driver's licenses and addresses.

12 32. Recently, Forbes writer Lee Mathews reported on Geico's similar
 13 unauthorized data disclosure wherein the hackers also targeted driver's license
 14 numbers, "Hackers harvest license numbers because they're a very valuable piece of
 15 information. A driver's license can be a critical part of a fraudulent, synthetic
 16 identity – which go for about \$1200 on the Dark Web. On its own, a forged license
 17 can sell for around \$200."¹¹

18 33. National credit reporting company, Experian, blogger Sue Poremba also
 19

20 ⁹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital
 21 Trends, Oct. 16, 2019, available at:
<https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited May 29, 2021).

21 ¹⁰ *Here's How Much Your Personal Information Is Selling for on the Dark Web*,
 22 Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>
 23 (last visited May 29, 2021).

24 ¹¹ Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), available at:
<https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658> (last visited
 25 May 29, 2021).

1 emphasized the value of driver's license to thieves and cautioned:

2 If someone gets your driver's license number, it is also
 3 concerning because it's connected to your vehicle registration
 4 and insurance policies, as well as records on file with the
 5 Department of Motor Vehicles, place of employment (that keep
 6 copy of your driver's license on file), doctor's office, government
 7 agencies, and other entities. Having access to that one number
 8 can provide an identity thief with several pieces of information
 they want to know about you. Next to your Social Security
 number, your driver's license is one of the most important pieces
 to keep safe from thieves.¹²

9 34. In fact, according to CPO Magazine, which specializes in news, insights
 10 and resources for data protection, privacy and cyber security professionals, "[t]o
 11 those unfamiliar with the world of fraud, driver's license numbers might seem like a
 12 relatively harmless piece of information to lose if it happens in isolation. Tim Sadler,
 13 CEO of email security firm Tessian, points out why this is not the case and why
 14 these numbers are very much sought after by cyber criminals: "It's a gold mine for
 15 hackers. With a driver's license number, bad actors can manufacture fake IDs,
 16 slotting in the number for any form that requires ID verification, or use the
 17 information to craft curated social engineering phishing attacks. . . . bad actors may
 18 be using these driver's license numbers to fraudulently apply for unemployment
 19 benefits in someone else's name, a scam proving especially lucrative for hackers as
 20 unemployment numbers continue to soar. . . . In other cases, a scam using these
 21 driver's license numbers could look like an email that impersonates the DMV,
 22 requesting the person verify their driver's license number, car registration or
 23 insurance information, and then inserting a malicious link or attachment into the
 24 email."

25
 26
 27 ¹² Sue Poremba, *What should I do If My Driver's License Number is Stolen?* (Oct. 24,
 28 2018), available at: <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/> (last visited May 29, 2021).

1 35. Drivers' license numbers have been taken from auto-insurance providers
 2 by hackers in other circumstances, indicating both that this particular form of PI is in
 3 high demand and also that Noblr knew or had reason to know that its security
 4 practices were of particular importance to safeguard consumer data.¹³

5 36. Once PI is sold, it is often used to gain access to various areas of the
 6 victim's digital life, including bank accounts, social media, credit card, and tax
 7 details. This can lead to additional PI being harvested from the victim, as well as PI
 8 from family, friends and colleagues of the original victim.

9 37. According to the FBI's Internet Crime Complaint Center (IC3) 2019
 10 Internet Crime Report, Internet-enabled crimes reached their highest number of
 11 complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to
 12 individuals and business victims.

13 38. Further, according to the same report, "rapid reporting can help law
 14 enforcement stop fraudulent transactions before a victim loses the money for good."
 15 Defendant did not rapidly report to Plaintiffs and Class Members that their PI had
 16 been stolen. It took Noblr almost four months to do so.

17 39. Victims of drivers' license number theft also often suffer unemployment
 18 benefit fraud, harassment in person or online, and/or experience financial losses
 19 resulting from fraudulently opened accounts or misuse of existing accounts.

20 40. Unauthorized data disclosures facilitate identity theft as hackers obtain
 21 consumers' PI and thereafter use it to siphon money from current accounts, open

23 ¹³ See United States Securities and Exchange Commission Form 8-K for INSU
 24 Acquisition Corp. II (Feb. 1, 2021),
 25 https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?_=1819035-01022021 (accessed Apr. 27, 2021) (announcing a
 26 merger with auto-insurance company MetroMile, Inc., an auto-insurer, which
 27 announced a drivers' license number Data Disclosure on January 19, 2021); Ron
 28 Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021)
 (describing a scam involving drivers' license numbers and Progressive Insurance).

1 new accounts in the names of their victims, or sell consumers' PI to others who do
 2 the same.

3 41. For example, the United States Government Accountability Office noted
 4 in a June 2007 report on data breaches (the "GAO Report") that criminals use PI to
 5 open financial accounts, receive government benefits, and make purchases and
 6 secure credit in a victim's name.¹⁴ The GAO Report further notes that this type of
 7 identity fraud is the most harmful because it may take some time for a victim to
 8 become aware of the fraud, and can adversely impact the victim's credit rating in the
 9 meantime. The GAO Report also states that identity theft victims will face
 10 "substantial costs and inconveniences repairing damage to their credit records . . .
 11 [and their] good name."¹⁵

12 **C. Noblr was on notice of the sensitivity and private nature of the PI it
 13 utilized for insurance quotes and its duty to safeguard it**

14 42. "Insurance companies are desirable targets for cyber attackers because
 15 they work with sensitive data."¹⁶ In fact, according to the Verizon 2020 Data Breach
 16 Investigations Report there were 448 confirmed data breaches in the financial and
 17 insurance industries.¹⁷

18 43. Noblr claims it "uses commercially reasonable and industry standard
 19 administrative, technical, personnel, and physical security measures designed to
 20

21 ¹⁴ See Government Accountability Office, *Personal Information: Data Breaches are
 22 Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full
 23 Extent is Unknown* (June 2007), available at
<http://www.gao.gov/assets/270/262899.pdf> (last visited May 29, 2021).

24 ¹⁵ *Id.*

25 ¹⁶ Data Protection Compliance for the Insurance Industry (October 7, 2020), available
 26 at: <https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry> (last visited May 29, 2021).

27 ¹⁷ Verizon 2020 Data Breach Investigations Report (2020), available at:
<https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf> (last visited May 29, 2021).

1 protect the information we collect about you from loss, theft, and unauthorized use,
 2 disclosure, or modification,” however, those safety and security measures were
 3 insufficient. And while Noblr states that the information is protected in an encrypted
 4 environment¹⁸, it was not. The weakness in Noblr’s system allowed access and
 5 ability to exfiltrate Plaintiffs’ and the Class Members’ addresses and driver’s license
 6 numbers.

7 **D. Noblr failed to comply with Federal Trade Commission requirements**

8 44. Federal and State governments have established security standards and
 9 issued recommendations to minimize unauthorized data disclosures and the resulting
 10 harm to individuals and financial institutions. The Federal Trade Commission
 11 (“FTC”) has issued numerous guides for businesses that highlight the importance of
 12 reasonable data security practices. According to the FTC, the need for data security
 13 should be factored into all business decision-making.¹⁹

14 45. In 2016, the FTC updated its publication, *Protecting Personal*
 15 *Information: A Guide for Business*, which established guidelines for fundamental
 16 data security principles and practices for business.²⁰ Among other things, the
 17 guidelines note businesses should properly dispose of personal information that is no
 18 longer needed; encrypt information stored on computer networks; understand their
 19 network’s vulnerabilities; and implement policies to correct security problems. The
 20 guidelines also recommend that businesses use an intrusion detection system to
 21 expose a breach as soon as it occurs; monitor all incoming traffic for activity
 22 indicating someone is attempting to hack the system; watch for large amounts of

23
 24¹⁸ *Id.*

25¹⁹ See Federal Trade Commission, *Start With Security* (June 2015), available at:
 26 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited May 29, 2021).

27²⁰ See Federal Trade Commission, *Protecting Personal Information: A Guide for*
 28 *Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 29, 2021).

1 data being transmitted from the system; and have a response plan ready in the event
 2 of a breach.²¹

3 46. Also, the FTC recommends that companies limit access to sensitive data;
 4 require complex passwords to be used on networks; use industry-tested methods for
 5 security; monitor for suspicious activity on the network; and verify that third-party
 6 service providers have implemented reasonable security measures.²²

7 47. Highlighting the importance of protecting against unauthorized data
 8 disclosures, the FTC has brought enforcement actions against businesses for failing
 9 to adequately and reasonably protect PI, treating the failure to employ reasonable
 10 and appropriate measures to protect against unauthorized access to confidential
 11 consumer data as an unfair act or practice prohibited by Section 5 of the Federal
 12 Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these
 13 actions further clarify the measures businesses must take to meet their data security
 14 obligations.²³

15 48. Through negligence in securing Plaintiffs’ and Class Members’ PI and
 16 allowing the thieves to utilize its instant quote website platform to obtain access and
 17 exfiltrate individuals’ PI, Noblr failed to employ reasonable and appropriate
 18 measures to protect against unauthorized access to Plaintiffs’ and the Class
 19 Members’ PI. Noblr’s data security policies and practices constitute unfair acts or
 20 practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the
 21 Gramm-Leach-Bliley Act (“GLB Act”), 15 U.S.C. § 6801.

22 **E. Plaintiffs’ attempts to secure their PI after the breach**

23 **Plaintiff Greenstein**

25 ²¹ *Id.*

26 ²² Federal Trade Commission, *Start With Security*, *supra* footnote 25.

27 ²³ Federal Trade Commission, *Privacy and Security Enforcement Press Releases*,
 28 available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Jan. 8, 2021).

1 49. In May 2021, Plaintiff Greenstein received notice from Noblr dated May
2 14, 2021 (“Notice Letter”). The Notice Letter informed him of the Unauthorized
3 Data Disclosure and that his driver’s license number and address may have been
4 accessed.

5 50. Plaintiff Greenstein researched his options to respond to the theft of his
6 driver’s license. He spent and continues to spend additional time reviewing his credit
7 monitoring service results and reports from other online resources concerning the
8 security of his identity and financial information. This is time Plaintiff Greenstein
9 otherwise would have spent performing other activities, such as his job and/or
10 leisurely activities for the enjoyment of life.

11 51. Plaintiff Greenstein has never knowingly transmitted unencrypted PI
12 over the internet or any other unsecured source. He deletes any and all electronic
13 documents containing his PI and destroys any documents that contain any of his PI,
14 or that may contain any information that could otherwise be used to compromise his
15 PI.

16 52. Plaintiff Greenstein suffered actual injury from having his PI exposed as
17 a result of the Unauthorized Data Disclosure including, but not limited to: (a)
18 damages to and diminution in the value of his PI—a form of intangible property; (b)
19 loss of his privacy; and (c) imminent and impending injury arising from the
20 increased risk of fraud and identity theft.

21 53. As a result of the Unauthorized Data Disclosure, Plaintiff Greenstein
22 will continue to be at heightened risk for financial fraud, future identity theft, other
23 forms of fraud, and the attendant damages, for years to come.

24 **Plaintiff Nelson**

25 54. In May 2021, Plaintiff Nelson received notice from Noblr dated May 14,
26 2021 (“Notice Letter”). The Notice Letter informed her of the Unauthorized Data
27 Disclosure and that her driver’s license number and address may have been
28 accessed.

1 55. As a result, Plaintiff Nelson notified her bank and financial planner of the
 2 Unauthorized Data Disclosure. She also contacted her local police department.

3 56. Plaintiff Nelson researched her options to respond to the theft of her
 4 driver's license. She spent and continues to spend additional time reviewing her
 5 credit monitoring service results and reports from other online resources concerning
 6 the security of her identity and financial information. This is time Plaintiff Nelson
 7 otherwise would have spent performing other activities, such as her job and/or
 8 leisurely activities for the enjoyment of life.

9 57. Plaintiff Nelson has never knowingly transmitted unencrypted PI over the
 10 internet or any other unsecured source. She deletes any and all electronic documents
 11 containing her PI and destroys any documents that contain any of her PI, or that may
 12 contain any information that could otherwise be used to compromise her PI.

13 58. Plaintiff Nelson suffered actual injury from having her PI exposed as a
 14 result of the Unauthorized Data Disclosure including, but not limited to: (a) damages
 15 to and diminution in the value of her PI—a form of intangible property; (b) loss of
 16 her privacy; and (c) imminent and impending injury arising from the increased risk
 17 of fraud and identity theft.

18 59. As a result of the Unauthorized Data Disclosure, Plaintiff Nelson will
 19 continue to be at heightened risk for financial fraud, future identity theft, other forms
 20 of fraud, and the attendant damages, for years to come.

21 **F. Plaintiffs and Class Members suffered damages**

22 60. Each of the Plaintiffs and Class Members are at risk for actual identity
 23 theft in addition to all other forms of fraud.

24 61. The ramifications of Noblr's failure to keep individuals' PI secure are
 25 long lasting and severe. Once PI is stolen, fraudulent use of that information and

1 damage to victims may continue for years.²⁴

2 62. The PI belonging to Plaintiffs and Class Members is private, valuable and
 3 is sensitive in nature as it can be used to commit a lot of different harms in the hands
 4 of the wrong people. Defendant Noblr failed to obtain Plaintiffs' and Class
 5 Members' consent to disclose such PI to any other person as required by applicable
 6 law and industry standards.

7 63. Noblr's inattention to the possibility that anyone, especially thieves with
 8 various pieces of individuals' PI, could obtain any individual's PI who utilized its
 9 front-facing instant quote platform left Plaintiff and Class Members with no ability
 10 to protect their sensitive and private information.

11 64. Noblr had the resources necessary to prevent the Unauthorized Data
 12 Disclosure, but neglected to adequately implement data security measures, despite
 13 its obligations to protect PI of the Plaintiffs and Class Members from unauthorized
 14 disclosure.

15 65. Had Noblr remedied the deficiencies in its data security systems and
 16 adopted security measures recommended by experts in the field, it would have
 17 prevented the intrusions into its systems and, ultimately, the theft of PI.

18 66. As a direct and proximate result of Noblr's actions and inactions,
 19 Plaintiffs and Class Members have been placed at an imminent, immediate, and
 20 continuing increased risk of harm from identity theft and fraud, requiring them to
 21 take the time which they otherwise would have dedicated to other life demands such
 22 as work and family in an effort to mitigate the actual and potential impact of the
 23 Unauthorized Data Disclosure on their lives.

24 67. The U.S. Department of Justice's Bureau of Justice Statistics found that

25
 26
 27 ²⁴ 2014 LexisNexis True Cost of Fraud Study, (August 2014), available at:
 28 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last visited May 29, 2021).

1 “among victims who had personal information used for fraudulent purposes, 29%
 2 spent a month or more resolving problems” and that “resolving the problems caused
 3 by identity theft [could] take more than a year for some victims.”²⁵

4 68. As a result of Noblr’s failures to prevent the Unauthorized Data
 5 Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at
 6 increased risk of suffering:

- 7 a. The compromise, publication, theft, and/or unauthorized use of their PI,
- 8 b. Out-of-pocket costs associated with the prevention, detection, recovery,
 and remediation from identity theft or fraud,
- 9 c. Lost opportunity costs and lost wages associated with efforts expended
 and the loss of productivity from addressing and attempting to mitigate the
 actual and future consequences of the Unauthorized Data Disclosure,
 including but not limited to efforts spent researching how to prevent,
 detect, contest, and recover from identity theft and fraud,
- 10 d. The continued risk to their PI, which remains in the possession of Noblr
 and is subject to further breaches so long as Noblr fails to undertake
 appropriate measures to protect the PI in its possession; and
- 11 e. Current and future costs in terms of time, effort, and money that will be
 expended to prevent, detect, contest, remediate, and repair the impact of
 the Unauthorized Data Disclosure for the remainder of the lives of
 Plaintiffs and Class Members.

12 69. In addition to a remedy for the economic harm, Plaintiffs and the Class
 13 Members maintain an undeniable interest in ensuring that their PI is secure, remains
 14 secure, and is not subject to further misappropriation and theft.

15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

²⁵ U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, available at: <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited May 29, 2021).

1 70. To date, other than providing 12 months of credit monitoring and identity
 2 protection services, Noblr does not appear to be taking any measures to assist
 3 Plaintiffs and Class Members other than simply telling them to do the following:

- 4 • “regularly review statements from your accounts”
- 5 • “periodically obtain your credit report”
- 6 • “remain vigilant with respect to viewing your account statements and
 7 credit reports”
- 8 • obtain a copy of a free credit report
- 9 • contact the FTC and/or the state Attorney General’s office to obtain
 10 additional information about avoiding identity theft

11 None of these recommendations, however, require Noblr to expend any effort to
 12 protect Plaintiffs’ and Class Members’ PI. It is also not clear that Noblr has made
 13 any determination that the credit monitoring and identity protection services are
 14 designed or adequate to ameliorate the specific harms of having an exposed driver’s
 15 license number and address.

16 71. Noblr’s failure to adequately protect Plaintiffs’ and Class Members’ PI
 17 has resulted in Plaintiffs and Class Members having to undertake these tasks, which
 18 require extensive amounts of time, calls, and, for many of the credit and fraud
 19 protection services, payment of money. Instead, as Noblr’s Notice indicates, it is
 20 putting the burden on Plaintiffs and Class Members to discover possible fraudulent
 21 activity and identity theft.

22 72. Noblr’s offer of 12 months of identity monitoring and identity protection
 23 services to Plaintiffs and Class Members is woefully inadequate. While some harm
 24 has begun already, the worst may be yet to come. There may be a time lag between
 25 when harm occurs versus when it is discovered, and also between when PI is
 26 acquired and when it is used.

27 **G. Noblr’s delay in identifying and reporting the breach caused additional
 28 harm**

73. The actual date Plaintiffs and the Class Members' PI was improperly exposed is unknown to Plaintiffs at this time, however, Noblr discovered the Unauthorized Data Disclosure on or about January 21, 2021, and it was not until almost four months later that Noblr began notifying those affected by the Unauthorized Data Disclosure, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Unauthorized Data Disclosure.

74. As a result of Noblr's delay in detecting and notifying Plaintiffs and Class Members of the Unauthorized Data Disclosure, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

CHOICE OF LAW

75. Defendant Noblr is headquartered in Marin County, California. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

76. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's California headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Unauthorized Data Disclosure were made from and in California. Finally, Defendant's breach of its duty—including to Plaintiffs and Class and Subclass Members—emanated from California.

77. It is appropriate to apply California law extraterritorially to the claims against Defendant in this case due to Defendant's significant contacts with California. Defendant is headquartered in California; the relevant decisions, actions, and omissions were made in California; and Defendant cannot claim to be surprised by application of California law to regulate its conduct emanating from California.

78. To the extent California law conflicts with the law of any other state that could apply to Plaintiffs' claims against Defendant, application of California law

1 would lead to the most predictable result, promote the maintenance of interstate
 2 order, simplify the judicial task, and advance the forum's governmental interest.

3 **CLASS ACTION ALLEGATIONS**

4 79. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs
 5 bring this action on behalf of themselves and the following proposed Nationwide
 6 Class (the "Class"), defined as follows:

7 All persons in the United States whose PI was compromised in
 8 the Unauthorized Data Disclosure announced by Noblr on or
 9 near May 14, 2021.

10 80. Excluded from the proposed Class are any officer or director of
 11 Defendant; any officer or director of any affiliate, parent, or subsidiary of Noblr;
 12 anyone employed by counsel in this action; and any judge to whom this case is
 13 assigned, his or her spouse, and members of the judge's staff.

14 81. **Numerosity.** Members of the proposed Class likely number in at least the
 15 tens of thousands and are thus too numerous to practically join in a single action.
 16 Membership in the Class is readily ascertainable from Defendant's own records.

17 82. **Commonality and Predominance.** Common questions of law and fact
 18 exist as to all proposed Class Members and predominate over questions affecting
 19 only individual Class Members. These common questions include:

- 20 a. Whether Defendant engaged in the wrongful conduct alleged herein,
- 21 b. Whether Defendant's inadequate data security measures were a cause of
 the Unauthorized Data Disclosure,
- 22 c. Whether Defendant owed a legal duty to Plaintiffs and the other Class
 Members to exercise due care in collecting, storing, and safeguarding their PI,
- 23 d. Whether Defendant negligently or recklessly breached legal duties owed
 to Plaintiffs and the other Class Members to exercise due care in collecting, storing,
 and safeguarding their PI,
- 24 e. Whether Defendant's online quote system auto-populated prospective

1 quotes with PI obtained from the records of Defendant or third parties without the
2 permission or consent of Plaintiffs and the Class,

3 f. Whether Plaintiffs and the Class are at an increased risk for identity theft
4 because of the data security breach,

5 g. Whether Defendant's conduct violated Cal. Bus. & Prof Code § 17200 *et*
6 *seq.*,

7 h. Whether Defendant failed to provide timely notice of the Unauthorized
8 Data Disclosure to Plaintiffs and Class Members in violation of California Civil
9 Code § 1798.82,

10 i. Whether Defendant violated the Drivers' Privacy Protection Act, 18
11 U.S.C. § 2724,

12 j. Whether Plaintiffs and the Class Members are entitled to actual,
13 statutory, or other forms of damages, and other monetary relief, and

14 k. Whether Plaintiffs and the Class Members are entitled to equitable relief,
15 including, but not limited to, injunctive relief and restitution.

16 83. Defendant engaged in a common course of conduct giving rise to the
17 legal rights sought to be enforced by Plaintiffs individually and on behalf of the
18 other Class Members. Similar or identical statutory and common law violations,
19 business practices, and injuries are involved. Individual questions, if any, pale by
20 comparison, in both quantity and quality, to the numerous questions that dominate
21 this action.

22 84. **Typicality:** Plaintiffs' claims are typical of the claims of the members of
23 the Class. All Class Members were subject to the Unauthorized Data Disclosure and
24 had their PI accessed by, used and/or disclosed to unauthorized third parties.
25 Defendant's misconduct impacted all Class Members in the same manner.

26 85. **Adequacy of Representation:** Plaintiffs are adequate representatives of
27 the Class because their interests do not conflict with the interests of the other Class
28 Members they seek to represent; they have retained counsel competent and

experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

86. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

**Violation of the Drivers' Privacy Protection Act (“DPPA”), 18 U.S.C. § 2724
(On behalf of Plaintiffs and the Nationwide Class)**

87. Plaintiffs incorporate the above allegations by reference.

88. The DPPA provides that “[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains.” 18 U.S.C. § 2724.

89. Under the DPPA, a ““motor vehicle record’ means any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.”” 18 U.S.C. § 2725(a). Drivers’ license numbers are motor vehicle records under the

1 DPPA.

2 90. Defendant obtains motor vehicle records from its customers.

3 91. Defendant also obtains motor vehicle records directly from state agencies
4 or through resellers who sell such records.

5 92. During the time period up until and including at least January 27, 2021,
6 PI, including drivers' license numbers, of Plaintiffs and Class Members, were
7 publicly available on Noblr's instant quote webpage and Noblr knowingly both used
8 and disclosed Plaintiffs' and members of the class's motor vehicle records for a
9 purpose not permitted by the DPPA pursuant to 18 U.S.C. §§ 2724 and 2721(b).

10 93. Through the Unauthorized Data Disclosure, Defendant disclosed motor
11 vehicle records for purposes not authorized by the DPPA.

12 94. Plaintiffs and putative Class Members are entitled to actual damages,
13 liquidated damages, punitive damages, attorneys' fees and costs.

14 **SECOND CAUSE OF ACTION**

15 **Negligence**

16 **(On behalf of Plaintiffs and the Nationwide Class)**

17 95. Plaintiffs incorporate the above allegations by reference.

18 96. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable
19 care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and
20 Class Members' PI from being compromised, lost, stolen, and accessed by
21 unauthorized persons. This duty includes, among other things, designing,
22 implementing, maintaining and testing its data security systems to ensure that
23 Plaintiffs' and Class Members' PI in Defendant's possession, or that could be
24 accessed by Defendant, was adequately secured and protected.

25 97. Defendant owed a duty of care to Plaintiffs and Members of the Class to
26 provide security, consistent with industry standards, to ensure that its systems and
27 networks adequately protected PI it stored, maintained, and/or obtained.

28 98. Defendant owed a duty of care to Plaintiffs and Members of the Class

1 because they were foreseeable and probable victims of any inadequate data security
 2 practices. Defendant knew or should have known of the inherent risks in having its
 3 systems auto-populate online quote requests with private PI and without the consent
 4 or authorization of the person whose PI was being provided.

5 99. Unbeknownst to Plaintiffs and Members of the Class, they were
 6 entrusting Defendant with their PI when Defendant obtained their PI from other
 7 businesses. Defendant had an obligation to safeguard their information and was in a
 8 position to protect against the harm suffered by Plaintiffs and Members of the Class
 9 as a result of the Unauthorized Data Disclosure.

10 100. Defendant's own conduct also created a foreseeable risk of harm to
 11 Plaintiffs and Class Members and their PI. Defendant's misconduct included failing
 12 to implement the systems, policies, and procedures necessary to prevent the
 13 Unauthorized Data Disclosure.

14 101. Defendant knew, or should have known, of the risks inherent in
 15 collecting and storing PI and the importance of adequate security. Defendant knew
 16 about – or should have been aware of - numerous, well-publicized unauthorized data
 17 disclosures affecting businesses, especially insurance and financial businesses, in the
 18 United States.

19 102. Defendant breached its duties to Plaintiffs and Class Members by failing
 20 to provide fair, reasonable, or adequate computer systems and data security to
 21 safeguard the PI of Plaintiffs and Class Members.

22 103. Because Defendant knew that a breach of its systems would damage
 23 thousands of individuals whose PI was inexplicably stored or was accessible,
 24 including Plaintiffs and Class Members, Defendant had a duty to adequately protect
 25 its data systems and the PI contained and/or accessible therein.

26 104. Defendant also had independent duties under state and federal laws that
 27 required Defendant to reasonably safeguard Plaintiffs' and Class Members' PI.

28 105. In engaging in the negligent acts and omissions as alleged herein, which

1 permitted thieves to access Noblr's systems that stored and/or had access to
2 Plaintiffs and Class Members' PI, Defendant violated Section 5 of the FTC Act,
3 which prohibits "unfair...practices in or affecting commerce," and the GLB Act.
4 This includes failing to have adequate data security measures and failing to protect
5 Plaintiffs' and the Class Members' PI.

6 106. Plaintiffs and the Class Members are among the class of persons Section
7 5 of the FTC and the GLB Act were designed to protect, and the injuries suffered by
8 Plaintiffs and the Class Members are the types of injury Section 5 of the FTC Act
9 and the GLB were intended to prevent.

10 107. Neither Plaintiffs nor the other Class Members contributed to the
11 Unauthorized Data Disclosure as described in this Complaint.

12 108. As a direct and proximate cause of Defendant's conduct, Plaintiffs and
13 Class Members have suffered and/or will suffer injury and damages, including but
14 not limited to: (i) the loss of the opportunity to determine for themselves how their
15 PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses
16 associated with the prevention, detection, and recovery from unauthorized use of
17 their PI; (iv) lost opportunity costs associated with effort expended and the loss of
18 productivity addressing and attempting to mitigate the actual and future
19 consequences of the Unauthorized Data Disclosure, including but not limited to
20 efforts spent researching how to prevent, detect, contest and recover from tax fraud
21 and identity theft; (v) costs associated with placing freezes on credit reports; (vi)
22 anxiety, emotional distress, loss of privacy, and other economic and non-economic
23 losses; (vii) the continued risk to their PI, which remains in Defendant's possession
24 (and/or Defendant has access to) and is subject to further unauthorized disclosures so
25 long as Defendant fails to undertake appropriate and adequate measures to protect
26 the PI in its continued possession; and, (viii) future costs in terms of time, effort and
27 money that will be expended to prevent, detect, contest, and repair the inevitable and
28 continuing consequences of compromised PI.

THIRD CAUSE OF ACTION

Violation of the California's Unfair Competition Law

Cal. Bus. & Prof. Code § 17200, *et seq.*

(Brought by Plaintiffs and the Nationwide Class)

109. Plaintiffs incorporate the above allegations by reference.

110. By reason of the conduct alleged herein, Defendant Noblr engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

111. Defendant stored and/or provided access to the PI of Plaintiffs and all Class Members in its computer systems.

112. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiffs' and all Class Members' PI secure and prevented the loss or misuse of that PI.

Unlawful Business Practices

113. Defendant violated the DPPA, Section 5(a) of the FTC Act, the GLB Act and California Civil Code § 1798.81.5(b) by failing to implement and maintain reasonable and appropriate security measures or follow industry standards for data security, and by failing to timely notify Plaintiffs and all Class Members of the Unauthorized Data Disclosure.

114. If Defendant had complied with these legal requirements, Plaintiffs and the Class Members would not have suffered the damages related to the Unauthorized Data Disclosure, and Defendant's notification of it.

115. Plaintiffs and all Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiffs and all Class Members' PI was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the

1 hacked information is of tangible value. Plaintiffs and all Class Members have also
 2 suffered consequential out of pocket losses for procuring credit freeze or protection
 3 services, identity theft monitoring, and other expenses relating to identity theft losses
 4 or protective measures.

5 **Unfair Business Practices**

6 116. Defendant engaged in unfair business practices under the “balancing
 7 test.” The harm caused by Defendant’s actions and omissions, as described in detail
 8 above, greatly outweigh any perceived utility. Indeed, none of Defendant’s actions
 9 or inactions can be said to have had any utility at all. Defendant’s failures were
 10 clearly injurious to Plaintiffs and all Class Members, directly causing the harms
 11 alleged below.

12 117. Defendant also engaged in unfair business practices under the “tethering
 13 test.” Defendant’s actions and omissions, as described in detail above, violated
 14 fundamental public policies expressed by the California Legislature. See, e.g., Cal.
 15 Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of
 16 privacy in information pertaining to them The increasing use of computers . . .
 17 has greatly magnified the potential risk to individual privacy that can occur from the
 18 maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the
 19 intent of the Legislature to ensure that personal information about California
 20 residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the
 21 Legislature that this chapter [including the Online Privacy Protection Act] is a matter
 22 of statewide concern.”). Defendant’s acts and omissions thus amount to a violation
 23 of the law.

24 118. Defendant engaged in unfair business practices under the “FTC test.” The
 25 harm caused by Defendant’s actions and omissions, as described in detail above, is
 26 substantial in that it affects tens of thousands of Class Members and has caused
 27 those persons to suffer actual harms. Such harms include a substantial risk of
 28 identity theft, disclosure of Plaintiffs’ and all Class Members’ PI to third parties

1 without their consent, diminution in value of their PI, consequential out of pocket
 2 losses for procuring credit freeze or protection services, identity theft monitoring,
 3 and other expenses relating to identity theft losses or protective measures. This harm
 4 continues given the fact that Plaintiffs' and all Class Members' PI remains in
 5 Defendant's possession, without adequate protection, and is also in the hands of
 6 those who obtained it without their consent. Defendant's actions and omissions
 7 violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n)
 8 (defining "unfair acts or practices" as those that "cause[] or [are] likely to cause
 9 substantial injury to consumers which [are] not reasonably avoidable by consumers
 10 themselves and not outweighed by countervailing benefits to consumers or to
 11 competition"); see also, e.g., *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File
 12 No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate
 13 measures to secure personal information collected violated § 5(a) of FTC Act).

14 119. Plaintiffs and all Class Members suffered injury in fact and lost money or
 15 property as the result of Defendant's unfair business practices. Plaintiffs and all
 16 Class Members' PI was taken and is in the hands of those who will use it for their
 17 own advantage, or is being sold for value, making it clear that the hacked
 18 information is of tangible value. Plaintiffs and all Class Members have also suffered
 19 consequential out of pocket losses for procuring credit freeze or protection services,
 20 identity theft monitoring, and other expenses relating to identity theft losses or
 21 protective measures.

22 120. As a result of Defendant's unlawful and unfair business practices in
 23 violation of the UCL, Plaintiffs and all Class Members are entitled to equitable and
 24 injunctive relief, including restitution or disgorgement.

25 **FORTH CAUSE OF ACTION**

26 **Declaratory and Injunctive Relief**

27 **(Brought by Plaintiffs and the Nationwide Class)**

28 121. Plaintiffs incorporate the above allegations by reference.

1 122. This Count is brought under the federal Declaratory Judgment Act, 28
2 U.S.C. §2201.

3 123. As previously alleged, Plaintiffs and Class Members had a reasonable
4 expectation that companies such as Defendant, who could access their PI through
5 automated systems, would provide adequate security for that PI.

6 124. Defendant owes a duty of care to Plaintiffs and Class Members requiring
7 it to adequately secure PI.

8 125. Defendant still possesses PI regarding Plaintiffs and Class Members.

9 126. Since the Unauthorized Data Disclosure, Defendant has announced few if
10 any changes to its data security infrastructure, processes, or procedures to fix the
11 vulnerabilities in its computer systems and/or security practices which permitted the
12 Unauthorized Data Disclosure to occur and, thereby, prevent further attacks.

13 127. The Unauthorized Data Disclosure has caused actual harm because of
14 Defendant's failure to fulfill its duties of care to provide security measures to
15 Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of
16 additional or further harm due to the exposure of their PI and Defendant's failure to
17 address the security failings that lead to such exposure.

18 128. There is no reason to believe that Defendant's security measures are any
19 more adequate now than they were before the Unauthorized Data Disclosure to meet
20 Defendant's legal duties.

21 129. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing
22 security measures do not comply with its duties of care to provide adequate security,
23 and (2) that to comply with its duties of care, Defendant must implement and
24 maintain reasonable security measures, including, but not limited to:

25 a. Ordering that Defendant engage third-party security auditors/penetration
26 testers as well as internal security personnel to conduct testing, including simulated
27 attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and
28 ordering Defendant to promptly correct any problems or issues detected by such

1 third-party security auditors,

2 b. Ordering that Defendant engage third-party security auditors and internal
3 personnel to run automated security monitoring,

4 c. Ordering that Defendant audit, test, and train its security personnel
5 regarding any new or modified procedures,

6 d. Ordering that Defendant not transmit PI via unencrypted email and not be
7 permitted to put PI as part of its source code or otherwise be available on its instant
8 quote webpage,

9 e. Ordering that Defendant not store or make accessible PI in any publicly
10 facing website,

11 f. Ordering that Defendant purge, delete, and destroy in a reasonably secure
12 manner customer data not necessary for its provisions of services,

13 g. Ordering that Defendant conduct regular computer system scanning and
14 security checks,

15 h. Ordering that Defendant routinely and continually conduct internal
16 training and education to inform internal security personnel how to identify and
17 contain a disclosure when it occurs and what to do in response to a breach; and

18 i. Ordering Defendant to meaningfully educate its current, former, and
19 prospective employees about the threats they face as a result of the loss of their PI to
20 third parties, as well as the steps they must take to protect themselves.

21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly
23 situated, respectfully request that the Court enter an order:

24 a. Certifying the proposed Class as requested herein,

25 b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class
26 Counsel,

27 c. Finding that Defendant engaged in the unlawful conduct as alleged herein,

28 d. Granting injunctive relief requested by Plaintiffs, including but not limited to,

1 injunctive and other equitable relief as is necessary to protect the interests of
2 Plaintiffs and Class Members, including but not limited to an order:

- 3 i. prohibiting Noblr from engaging in the wrongful and unlawful acts
4 described herein,
- 5 ii. requiring Noblr to protect, including through encryption, all data
6 collected through the course of its business in accordance with all
7 applicable regulations, industry standards, and federal, state or local
8 laws,
- 9 iii. requiring Noblr to delete, destroy, and purge the personal information
10 of Plaintiffs and Class Members unless Noblr can provide to the Court
11 reasonable justification for the retention and use of such information
12 when weighed against the privacy interests of Plaintiffs and Class
13 Members,
- 14 iv. requiring Noblr to implement and maintain a comprehensive
15 Information Security Program designed to protect the confidentiality
16 and integrity of the personal information of Plaintiffs and Class
17 Members' personal information,
- 18 v. prohibiting Noblr from maintaining Plaintiffs' and Class Members'
19 personal information on a cloud-based database,
- 20 vi. requiring Noblr to engage independent third-party security
21 auditors/penetration testers as well as internal security personnel to
22 conduct testing, including simulated attacks, penetration tests, and
23 audits on Noblr's systems on a periodic basis, and ordering Noblr to
24 promptly correct any problems or issues detected by such third-party
25 security auditors,
- 26 vii. requiring Noblr's to engage independent third-party security auditors
27 and internal personnel to run automated security monitoring,
- 28 viii. requiring Noblr to audit, test, and train its security personnel regarding

- any new or modified procedures,
- ix. requiring Noblr to conduct regular database scanning and securing checks,
- x. requiring Noblr to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiffs and Class Members,
- xi. requiring Noblr to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,
- xii. requiring Noblr to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Noblr's policies, programs, and systems for protecting personal information,
- xiii. requiring Noblr to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Noblr's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,
- xiv. requiring Noblr to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,
- xv. requiring Noblr to design, maintain, and test its computer systems to

1 ensure that PI in its possession is adequately secured and protected,

2 xvi. requiring Noblr disclose any future data disclosures in a timely and

3 accurate manner; and

4 xvii. requiring Defendant to provide ongoing credit monitoring and identity

5 theft repair services to Class Members.

6 e. Awarding Plaintiffs and Class Members damages,

7 f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest

8 on all amounts awarded,

9 g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and

10 expenses; and

11 h. Granting such other relief as the Court deems just and proper.

12 **DEMAND FOR JURY TRIAL**

13 Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a
14 trial by jury as to all matters so triable.

15
16 Dated: June 11, 2021

17 /s/ Gayle M. Blatt
18 GAYLE M. BLATT

19 **CASEY GERRY SCHENK**
20 **FRANCAVILLA BLATT &**
21 **PENFIELD, LLP**
22 David S. Casey, Jr.
23 *dcasey@cglaw.com*
24 Gayle M. Blatt
25 *gmb@cglaw.com*
26 P. Camille Guerra
27 *camille@cglaw.com*
28 110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

29
30 Kate M. Baxter-Kauf (MN #0392037)

1 Karen Hanson Riebel (MN #0219770)
2 **LOCKRIDGE GRINDAL NAUEN**
3 **P.L.L.P.**
4 100 Washington Avenue South
5 Suite 2200
6 Minneapolis, MN 55401
7 Telephone: (612) 339-6900
8 Facsimile: (612) 339-0981
9 kmbaxter-kauf@locklaw.com
10 khriebel@locklaw.com

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28